BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

KONINKRIJK DER NEDERLANDEN

Bureau voor de Industriële Eigendom

Hierbij wordt verklaard, dat in Nederland op 10 januari 2003 onder nummer 1022348,

ten name van:

INTEGRATED ENGINEERING B.V.

te Amsterdam

een aanvrage om octrooi werd ingediend voor:

"SmartTOUCH2",

onder inroeping van een recht van voorrang, gebaseerd op de in Nederland op

12 september 2002 onder nummer 1021441 ingediende aanvrage om octrooi, en

dat de hieraan gehechte stukken overeenstemmen met de oorspronkelijk ingediende stukken.

Rijswijk, 26 februari 2003

De Directeur van het Bureau voor de Industriële Eigendom,
voor deze,

Mw. M.M. Enhus

1022348

SMARTTOUCH

Door aanvraagster (en/of daarmee gelieerde bedrijven) worden reeds geruime tijd systemen voor toegangscontrole en/of aanwezigheidsregistratie op de markt gebracht. Naar verwachting zal de vraag naar dergelijke apparatuur toenemen vanwege de steeds stringentere eisen die in de Westerse wereld en daarbuiten aan toegangscontrole en dergelijke worden gesteld.

Het bedrijf Bioscrypt Inc. brengt electronica op de markt die is voorzien van aftastmiddelen voor het aftasten van een vingerafdruk van een individu.

De onderhavige uitvinding verschaft een systeem volgens een of meer van de bijgevoegde conclusies.

Bij voorkeur wordt bij het systeem volgens de onderhavige uitvinding gebruik gemaakt van een zogeheten Smartcard waarop een geïntegreerd circuit of chip op een kaart is aangebracht, terwijl in het huis electronica van de Mifare techniek van Philips semiconductors is aangebracht.

Bij toegangscontrole wordt een Smartcard voor de Mifare electronica gehouden, wordt vervolgens een vingerafdruk op de sensormiddelen gelegd, waarna bijvoorbeeld een deur wordt geopend indien de gegevens juist zijn.

Dankzij de onderhavige uitvinding kan met behulp van een afzonderlijke Smartcard de Mifare electronica in een configuratie-of programmeermodus worden geplaatst, waarna het mogelijk wordt de gegevens van een vingerafdruk op de Smartcard van de gebruiker te laden. Problemen met privacywetgeving kunnen dankzij deze techniek worden vermeden, daar een vingerafdruk slechts op de Smartcard behoeft te worden opgeslagen. Voorts kan met behulp van dergelijke kaart de electronica in het huis in een gewenste configuratie worden gebracht, bijvoorbeeld afhankelijk van de

aanwezige omgeving van electronica, netwerk, hardware en/of software.

Verdere voordelen kenmerken en details van de onderhavige uitvinding worden verduidelijkt aan de hand van de navolgende beschrijving van een voorkeursuitvoeringsvorm daarvan met verwijzing naar de bijgevoegde figuur die een voorkeursuitvoeringsvorm vormt van een inrichting volgens de onderhavige uitvinding, die deel uitmaakt van het systeem volgens de onderhavige uitvindingen waarbij de werkwijze volgens onderhavige uitvinding kan worden toegepast.

Een inrichting 1 omvat een huis 2 waarin in het schuine bovenwand een vingerafdrukscaneenheid 3 bij voorkeur van de firma Bioscrypt is aangebracht.

In de verticale voorwand is een nabijheidsleeseenheid 4 bij voorkeur van het type Mifare aangebracht die via een electrische leiding is aangesloten op een door aanvraagster ontworpen en te fabriceren printed circuit board 5.

Op het printed circuit board is een tweede printed circuit board 6 die op zijn beurt is aangesloten op de eenheid 4, terwijl op de eerste printed circuit board een kabel 7 is aangesloten voor communicatie met de wandapparatuur.

De werking van het onderhoudsysteem zal duidelijk worden uit de navolgende eerste interne versie van een programmeer manual voor bovenbeschreven hardware die is te voorzien van geschikte software.

SmartTOUCH

1. General

The SmartTOUCH is a standard IE access control product. SmartTOUCH is a combination of a Mifare® proximity reader and a finger-scan module. SmartTOUCH offers a higher level of security: an authorised card alone is not sufficient to obtain access. The finger-scan of the user must match with the enrolled finger template on the Mifare® card. It is not possible to obtain access with someone else's card.

This document contains a brief explanation of the working of SmartTOUCH.

SmartTOUCH has three operating modes:

- *Access Mode:* granting access.
- *Enrolment Mode:* enrolling (storing a finger-scan on a Mifare® card).
- *Erase Mode:* erasing templates from a Mifare® card.

2. Access Mode: granting access

After powering up, the SmartTOUCH reader is in access mode. The green LED on the side of SmartTOUCH is on in this mode. The reader will now carry out the following functions:

- Read the LED and buzzer inputs. With these inputs an external device can control the red LED and the buzzer.
- Read a Mifare card. The following cards can be read by the SmartTOUCH:
  - Config Card: for changing the parameters of the reader.
  - Mifare card: a Mifare card with one or two finger-scan templates of the cardholder.
  - Enrol Card: for switching from access mode to enrolment mode.
  - Erase Card: for erasing the finger-scan templates of the Mifare card.
- Send the card number via the DTA- en CLK-output

Steps for obtaining access:

1. Hold the Mifare card with finger-template in front of the SmartTOUCH reader. The green LED is on as long the card is being read.
2. After the card has been read, the green LED turns off.
3. If a valid card is read the green LED of the SmartTOUCH starts blinking.

   This indicates that SmartTOUCH is ready to read the finger-scan. If the user doesn't present his/her finger within 5 to 6 seconds the green LED turns off and the Mifare® card must be read again.

   If the card is not read properly, or an invalid card is read, the SmartTOUCH buzzer will beep several times.
4. Place your finger on the scanner. The green LED is on during the finger-scan. After the finger has been scanned and checked, the green LED turns off.
5. If the template of the scanned finger matches with the template on the card, the card number is sent to the external system using the DTA and CLOCK data lines. After sending the card number, the SmartTOUCH beeps once.

Remark: Scanning and checking of the finger-scan template takes longer if two finger-scan templates are stored on the Mifare® card. If the first finger-scan template on the card doesn't match with the presented finger, the SmartTOUCH checks if the second template matches.

5. Hold the card in front of the reader within 5 to 6 seconds.
6. The green LED is on while the SmartTOUCH is erasing the Mifare® card.
7. The reader beeps once and returns to access mode after the card is completely erased.
8. If an error occurs during erasing, the SmartTOUCH beeps three times and returns to access mode.
9. If a Mifare® card is not presented within 5 to 6 seconds, the SmartTOUCH returns to the access mode.

5. Using the standard enrol card for storing two finger-scan templates

The standard enrol card which is shipped with the SmartTOUCH allows storing two finger-scan templates on the Mifare card. The procedure for storing one template is described in chapter 3. The procedure for storing two templates is as follows.

There is space available for two templates on each Mifare card. Adding a template to a card (enrolment) will store the template in one of these two positions, depending on whether there are 0, 1, or two templates already present. The new template will be stored as follows:

- 0 templates on card: On the first position on the card.
- 1 template on card: On the second position on the card
- 2 templates on card: On the second position on the card (this replaces the previous template in the second position).

The procedure for adding one or two templates is simply to follow the procedure described in chapter 3 once for one template, and twice for two templates.

If one wishes to replace the second finger-scan template on a card, carrying out the procedure in chapter 3 will do this. If one wishes to replace the first template, it is necessary to erase both templates using the erase card, and then enrol both the templates again.

6. Possible Errors

Error	Possible Cause
Green LED on side of reader does not turn on by power-up.	Hardware error
Reader does not accept SmartTOUCH Card.	-Card has no finger-scan template. -Card has no valid template. -Card has no IE card number data. -Distributor Code on card does not agree with Distributor Code in reader.
SmartTOUCH Card is read, but no card data is sent.	-Finger-scan template on card was not correctly read. -Finger-scan template on card does not agree with scanned finger.
Enrol Card is not accepted by reader.	-The Enrol Code[1] on the Enrol Card does not agree with the Enrol Code in the SmartTOUCH Reader. -The ECVC[2] on the Enrol Card is lower than the ECVC in the SmartTOUCH Reader.
The scanned finger is not accepted.	-The finger was removed from the scanner before the scan was completed. -The scan was not accurate enough.
The template cannot be written on the card.	-The card was too quickly removed from the reader. -There is not sufficient memory on the card. -The (encryption) key on the card is not the same as the key in the reader.
The Erase Card is not accepted.	-The Enrol Code on the Erase Card does not agree with the Enrol Code in the SmartTOUCH Reader. -The ECVC on the Erase Card is lower than the ECVC in the SmartTOUCH Reader.
The Mifare card is not correctly erased.	The card was too quickly removed from the reader. -The (encryption) key on the card is not the same as the key in the reader.

[1] The enrol card will only work on your SmartTOUCH. Using a unique Enrol Code ensures this.

[2] If an enrol card is lost, a new enrol card can be provided. This new enrol card will have the same enrol code, but a higher version number (ECVC).

Using the SmartTOUCH Reader Programming Manual

26 July, 2002 Version 1.0

1. General 3
2. Access Mode: granting access 3
3. Enrollment Mode: Storing a finger-scan template on a Mifare® card 4
4. Erase Mode: erasing finger-scan templates from a Mifare® card 4
5. Using the standard enroll card for storing two finger-scan templates 5
6. Possible Errors 6

SmartTOUCH

1. General

The SmartTOUCH is a standard IE access control product. SmartTOUCH is a combination of a Mifare® proximity reader and a finger-scan module. SmartTOUCH offers a higher level of security: an authorised card alone is not sufficient to obtain access. The finger-scan of the user must match with the enrolled finger template on the Mifare® card. It is not possible to obtain access with someone else's card.

This document contains a brief explanation of the working of SmartTOUCH.

SmartTOUCH has three operating modes:

- *Access Mode:* granting access.
- *Enrolment Mode:* enrolling (storing a finger-scan on a Mifare® card).
- *Erase Mode:* erasing templates from a Mifare® card.

2. Access Mode: granting access

After powering up, the SmartTOUCH reader is in access mode. The green LED on the side of SmartTOUCH is on in this mode. The reader will now carry out the following functions:

- Read the LED and buzzer inputs. With these inputs an external device can control the red LED and the buzzer.
- Read a Mifare card. The following cards can be read by the SmartTOUCH:
  - Config Card: for changing the parameters of the reader.
  - Mifare card: a Mifare card with one or two finger-scan templates of the cardholder.
  - Enrol Card: for switching from access mode to enrolment mode.
  - Erase Card: for erasing the finger-scan templates of the Mifare card.
- Send the card number via the DTA- en CLK-output.

Steps for obtaining access:

1. Hold the Mifare card with finger-template in front of the SmartTOUCH reader. The green LED is on as long the card is being read.
2. After the card has been read, the green LED turns off.
3. If a valid card is read the green LED of the SmartTOUCH starts blinking.

   This indicates that SmartTOUCH is ready to read the finger-scan. If the user doesn't present his/her finger within 5 to 6 seconds the green LED turns off and the Mifare® card must be read again.

   If the card is not read properly, or an invalid card is read, the SmartTOUCH buzzer will beep several times.
4. Place your finger on the scanner. The green LED is on during the finger-scan. After the finger has been scanned and checked, the green LED turns off.
5. If the template of the scanned finger matches with the template on the card, the card number is sent to the external system using the DTA and CLOCK data lines. After sending the card number, the SmartTOUCH beeps once.

Remark: Scanning and checking of the finger-scan template takes longer if two finger-scan templates are stored on the Mifare® card. If the first finger-scan template on the card doesn't match with the presented finger, the SmartTOUCH checks if the second template matches.

3. Enrolment Mode: Storing a finger-scan template on a Mifare® card

The enrolment mode is used for enrolling (storing) a finger-scan on the Mifare® card. A valid enrol Card is needed to switch from the default access mode to the enrolment mode. If the SmartTOUCH is in the enrolment mode the orange LED to the side of the reader is on and the green LED on the Mifare reader blinks.

Steps for storing a finger-scan template on a Mifare® card:

1. Begin with the SmartTOUCH in the default access mode (the green LED on the side of the SmartTOUCH is on).
2. Present a valid enrol-card to the reader. As long the card is being read the green LED is on.
3. If the card is properly read, the green LED turns off.
4. After a valid enrol-card is read, the green LED on the side of the SmartTOUCH turns off, the green LED on the reader starts blinking, and the orange LED on the side of the reader turns on. This indicates that the SmartTOUCH is in the enrol mode.
5. Place your finger on the scanner. While the finger is being scanned and the quality of the scan is being checked, the green LED is on.
6. After a correct scan, the SmartTOUCH beeps ones. After an incorrect scan, the SmartTOUCH beeps three times. After an incorrect scan the green LED starts blinking again and the finger can again be placed on the scanner.
7. After a correct scan, the green LED of the reader turns off and the red and orange LED on the side of the SmartTOUCH turn. This indicates that the card being enrolled must be presented to the SmartTOUCH in order to write the scanned finger-template on the card. If the user doesn't present the card within 5 to 6 seconds the reader beeps three times and the SmartTOUCH reverts to the start of the enrolment mode (the green LED of the SmartTOUCH starts blinking and only the orange LED on the side of the reader is on).
8. If the user presents the Mifare® card to the reader, the finger-scan is written to the card. During writing the green LED of the SmartTOUCH is on.
9. If the data is successfully written to the card, the reader beeps once and the reader returns to the enrolment mode. If the data is not successfully written, the reader beeps three times and returns to the enrolment mode.

Remark: While the SmartTOUCH is in the enrolment mode, more Mifare® cards can be enrolled. To return to the access mode a valid enrol card must be presented to the reader.

It is also possible to store two finger-scan templates on a card. See section 5 for more information on this subject.

4. Erase Mode: erasing finger-scan templates from a Mifare® card

The erase mode is used for erasing all stored finger-scan templates from a Mifare® card. A valid erase-card is needed to switch from the access mode to the erase mode. If the SmartTOUCH is in the erase mode, the red LED on the side of the SmartTOUCH is on and the green LED of the reader blinks.

Steps for erasing a Mifare® card:

1. Begin with the SmartTOUCH in the default access mode.
2. Present a valid erase card to the reader. While the card is being read, the green LED is on.
3. After the card has been read, the green LED turns off.
4. If a valid card has been read, the green LED on the side of the reader turns off and the red LED turns on. The green LED on the side of the reader turns on and the green LED of the SmartTOUCH starts blinking. This indicates that a Mifare® card can be erased.

5. Hold the card in front of the reader within 5 to 6 seconds.
6. The green LED is on while the SmartTOUCH is erasing the Mifare® card.
7. The reader beeps once and returns to access mode after the card is completely erased.
8. If an error occurs during erasing, the SmartTOUCH beeps three times and returns to access mode.
9. If a Mifare® card is not presented within 5 to 6 seconds, the SmartTOUCH returns to the access mode.

5. Using the standard enrol card for storing two finger-scan templates

The standard enrol card which is shipped with the SmartTOUCH allows storing two finger-scan templates on the Mifare card. The procedure for storing one template is described in chapter 3. The procedure for storing two templates is as follows.

There is space available for two templates on each Mifare card. Adding a template to a card (enrolment) will store the template in one of these two positions, depending on whether there are 0, 1, or two templates already present. The new template will be stored as follows:

- 0 templates on card: On the first position on the card.
- 1 template on card: On the second position on the card
- 2 templates on card: On the second position on the card (this replaces the previous template in the second position).

The procedure for adding one or two templates is simply to follow the procedure described in chapter 3 once for one template, and twice for two templates.

If one wishes to replace the second finger-scan template on a card, carrying out the procedure in chapter 3 will do this. If one wishes to replace the first template, it is necessary to erase both templates using the erase card, and then enrol both the templates again.

De ConfigKaarten van IE Keyprocessor

I. Introductie

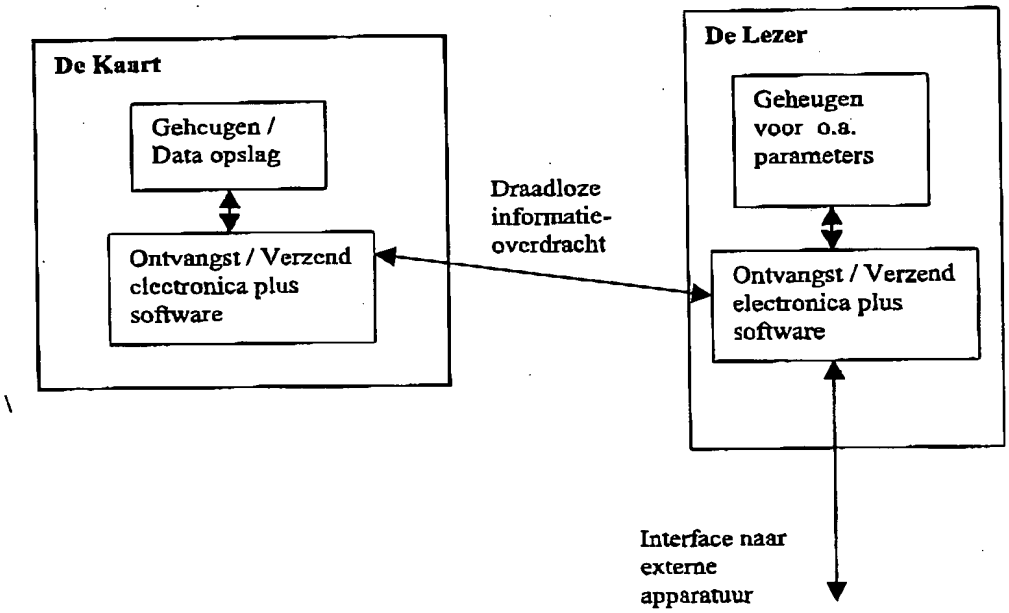
De ConfigKaart van IE Keyprocessor wordt gebruikt om de door IE Keyprocessor zelf ontwikkelde Mifare® lezers te voorzien van informatie (parameters) die bepaald hoe de lezer functioneert. Ook kan een ConfigKaart gebruikt worden om de werking van de SmartTOUCH lezer te programmeren. De werking van de ConfigKaart en een overzicht van de mogelijke instellingen van de lezers wordt gegeven na een korte omschrijving van de Mifare® lezer en de Mifare® kaart zelf. In hoofdstuk III wordt de werking van de Configkaart in combinatie met SmartTOUCH uitgelegd.

A. Mifare

De Mifare technologie is een gepatenteerde ontwikkeling van Philips die bedoeld is om informatie op een draagbare medium (bijvoorbeeld een kaart) contactloos te kunnen bewaren en lezen. Het draagbare medium zelf bevat altijd een chip waar in de gegevens bewaard worden en elektronica om met de buitenwereld (de lezer) te kunnen communiceren. Hoewel deze elektronica vaak in een kaart geplaatst wordt, is het mogelijk om die ook in een andere vorm of omgeving te monteren. In dit stuk zullen wij Het draagbare medium "de kaart" noemen.

De lezer heeft als functie de gegevens van de kaart te benaderen (lezen) en daarna door te geven aan een extern systeem, of de gegevens verkregen van een extern systeem op een kaart te zetten (schrijven).

Hieronder ziet u de werking van de kaart en de lezer schematisch weergegeven:



Tekening 1 : Schematische Werking Mifare Kaart en Lezer

B. Instelbare Lezers

Hoewel de werking van de lezer, zoals hierboven weergegeven, redelijk simpel lijkt, zijn er veel verschillende eisen die gesteld worden aan de functionaliteit van de lezer afhankelijk van de specifieke toepassing. Zelfs binnen een toepassing is het vaak noodzakelijk om lezers met andere informatie en functionaliteit te voorzien.

Bijvoorbeeld, als de kaart in een toegangscontrole toepassing gebruikt wordt, kan het noodzakelijk zijn dat kaarten van een klant überhaupt niet gelezen mogen worden bij een andere klant. Dit kan men verwezenlijken door de kaarten met verschillende "cryptografische sleutels" te beveiligen. Alleen als de lezer de goede sleutel (als parameter) heeft, kan hij de kaart lezen. Het kan ook zijn dat een klant een extern systeem gebruikt die een Wiegand protocol verwacht terwijl een andere klant een Magstripe protocol wenst.

De lezers van IE Keyprocessor zijn zodanig ontworpen dat vele van de verschillende eisen die gesteld worden aan de functionaliteit van de lezer door middel van "parameters" veranderd kunnen worden. In andere woorden, de werking van de lezer veranderd als een parameter wordt veranderd. Deze parameters worden opgeslagen in de geheugen van de lezer zelf zo dat deze instelling maar één keer hoeft te gebeuren.

Vroeger werden deze parameters door middel van een elektrische verbinding geladen in de lezer. Hiervoor was het noodzakelijk om de lezer aan te sluiten op een apparaat zoals een draagbare computer.

II. De ConfigKaart

De ConfigKaart is een standaard Mifare kaart voorzien van parameters die de werking van de lezer beïnvloeden. Door gebruik te maken van zo'n ConfigKaart is het mogelijk om, onder andere, logistieke kosten te verminderen door alleen standaard lezers te leveren (klanten hebben zelf een ConfigKaart waarmee ze de lezers kunnen programmeren), voorraadbeheer te vereenvoudigen omdat een lezer vele verschillende toepassingen ondersteund, en de servicekosten te minimaliseren doordat monteurs maar een lezertype moet hebben die makkelijk omgeprogrammeerd kan worden.

A. Werking Configkaart met Lezer

Lezers kunnen in twee verschillende modes functioneren: 3964-mode of standalone. In de 3964 mode wordt het functioneren van de lezer gecontrolleerd door een extern systeem, waardoor het inlezen van een Configkaart in deze mode alleen mogelijk is bij opstarten. In standalone mode kan de Configkaart gelezen worden bij het opstarten van de lezer maar ook tijdens normale operatie. Normale operatie betekent dat de lezer kaarten leest en de data op de kaart (of een gedeelte daarvan) doorgeeft aan een extern systeem.

1. Lezen van Configkaart bij Power-up

Direct na het opstarten van de lezer (het maakt niet uit of de lezer in 3964-mode of in standalone-mode staat) probeert de lezer 1 seconde lang een ConfigCard uit te lezen. Deze periode van 1 seconde wordt aangegeven door beide leds aan te zetten.

Als in deze periode geen ConfigCard wordt uitgelezen, gaat de lezer verder met zijn normale operatie. Dit betekent dat een lezer in 3964-mode alleen geconfigureerd kan worden met een ConfigCard bij een power-up.

Na het uitlezen van een ConfigCard wordt de lezer gereset om de parameters actief te maken!

2. Lezen van Configkaart in Standalone mode

Een mifarelezer in de standalonemode scant allereerst sector 0 op een eventuele MAD (Mifare Application Directory). Een MAD geeft aan in welke sector van de kaart wat voor informatie (voor welke applicatie) staat. Zo heeft iedere mifare applicatie zijn eigen identifier (AID):

IE toegangscontrole applicatie: AID = 0x482a

IE ConfigCard applicatie: AID = 0x0141

De volgende situaties kunnen voorkomen:

- De lezer leest een kaart met AID = 0x482a. De lezer weet dan waar het standaard IE-blok met toegangscontrole informatie op de kaart staat.
- De lezer leest een kaart met AID = 0x0141. De lezer weet dan dat deze kaart een ConfigCard is en weet ook meteen waar de parameter-informatie op de kaart staat.
- De lezer leest een kaart zonder AID. De lezer probeert dan het door de parameters aangegeven blok uit te lezehhn. Dit kan overigens geen ConfigCard zijn.

Na het uitlezen van een ConfigCard wordt de lezer gereset om de parameters actief te maken!

B. Lezergedrag tijdens lezen van Configkaart

Hieronder wordt beschreven hoe de gebruiker aan de leds en de buzzer kan waarnemen wat de status van de lezer is;

-bij power-up knippert het rode ledje 2x in een periode van 2 seconden; dit betekent dat de monitor geactiveerd kan worden. Wordt de monitor niet geactiveerd dan start de lezer door naar het applicatieprogramma.

-het applicatieprogramma start met het laden van de parameters uit de permanente geheugen; de tijd die hiervoor nodig is, hangt af van de hoeveelheid parameterdata in flashbank0. Vervolgens gaan beide leds voor een periode van 1 seconde aan om aan te geven dat de lezer probeert een ConfigCard uit te lezen.

-het lezen van een ConfigCard: op het moment dat de lezer een ConfigCard aangeboden krijgt (in standalone-mode of bij de power-up) en ziet dat het een ConfigCard is dan gaat het groene ledje aan (en het rode ledje gaat uit als deze aan was). Zolang de lezer bezig is met het lezen en verwerken van de ConfigCard blijft het groene ledje aan.

-Een ConfigCard kan geaccepteerd of niet geaccepteerd worden:

1. als een ConfigCard geaccepteerd is (als hij volledig gelezen en verwerkt is), geeft de lezer allereerst een buzzersignaal en vervolgens gaat het groene ledje voor een periode van 1 seconde snel knipperen. De lezer wordt nu gereset en start weer bij de monitor.
2. als een ConfigCard niet geaccepteerd is, gaat het groene ledje uit en geeft de lezer drie korte buzzersignalen. Vervolgens gaat het rode ledje voor een periode van 1 seconde snel knipperen.

Een ConfigCard kan door de volgende redenen niet geaccepteerd worden:

1. als de sleutels van de kaart en de lezer niet overeen komen;
2. als CCVC in de lezer en de kaart niet overeen komen;
3. of als er een andere fout optreedt tijdens het lezen van de kaart.

C. Beveiliging ConfigKaart

a) Keys

De default sleutel voor het uitlezen van een ConfigCard is een door IE bepaalde geheime sleutel. Omdat deze sleutel in elke lezer (die van het productiebedrijf komt) hetzelfde is kan klant x met zijn ConfigCard een lezer van klant y omprogrammeren, wat zeer ongewenst is.

Het is dus mogelijk om de sleutel waarmee de ConfigCard uitgelezen wordt aan te passen met de parameter KACC. Let wel op dat deze sleutel gecrypt in de lezer wordt geladen.

De lezer leest de gehele ConfigCard met de default b-sleutel tenzij de parameter KACC bestaat; dan wordt de kaart met deze sleutel gelezen.

b) Versienummer / Versioncontrol

ConfigCardversioncontrol is een door de lezer ondersteunde beveiliging tegen het uitlezen van een oudere ConfigCard. Voor het gebruik van deze versioncontrol moet op de ConfigCard een versienummer staan. Dit versienummer wordt als parametervariabele (CCVC) op de kaart gezet: bv. CCVC=1.

Elke ConfigCard met versioncontrol heeft dus een versienummer die door de gebruiker bij het programmeren van de ConfigCard opgegeven kan worden (als parameter). Met dit versienummer kan de gebruiker een oudere kaart met een ouder versienummer ongeldig maken. De lezer onthoudt namelijk het versienummer van de laatst gelezen ConfigCard en accepteert alleen nog maar een ConfigCard met hetzelfde of een nieuwer versienummer.

Als de gebruiker geen gebruik wilt maken van ConfigCardversioncontrol hoeft hij niets te doen; als de parametervariabele voor versioncontrol niet gezet is en dus op 0 staat, is de optie uitgeschakeld.

III. De ConfigKaart met SmartTOUCH

De SmartTOUCHReader is een standaard produkt van IE op het gebied van toegangscontrole. De SmartTOUCHReader is een combinatie van een IE Keyprocessor Mifare lezer en een FingerScan module (MV1200 van BioScript).

De SmartTOUCHReader biedt een nog hoger nivo van veiligheid; een geauthentiseerde kaart alleen is niet voldoende om toegang te krijgen, ook de vingerafdruk van de gebruiker van de kaart moet overeenkomen met op de kaart opgeslagen vingerafdruk. Het is dus niet mogelijk om een kaart van iemand anders te gebruiken voor het verkrijgen van toegang.

A. Werking SmartTouch

In de normale mode van de lezer, wacht de lezer op een Mifarekaart waarop er een fingerscan profiel staat van de houder van de kaart. Nadat de kaart gelezen is, moet de houder van de kaart zijn of haar vinger op de fingerscan lezer plaatsen. Daarna worden de fingerscan profielen vergeleken. Als ze met elkaar overeenkomen geeft de lezer de toegangsinformatie door aan het extern systeem.

In deze situatie gaan we er vanuit dat de fingerscan profiel al op de kaart is. Het is natuurlijk ook noodzakelijk om een manier te hebben om het profiel op de kaart te schrijfen. Dit is mogelijk door gebruik te maken van de SmartTOUCH zelf, nadat een geauthoriseerde Enrollkaart gelezen is.

Om ervoor te zorgen dat de fingerscan profiel gewist kan worden, kan men de SmartTOUCH in "wis mode" gezet worden d.m.v. een WisKaart. Daarna wordt de de fingerscan profiel(en) op de volgende voorgehouden Mifarekaart gewist.

De functionaliteit van de SmartTOUCHReader is dus in drie modes op te splitsen:

- *Access Mode:* het verlenen van toegang.
- *Enroll Mode:* het inleren van een kaart.
- *Erase Mode:* het wissen van een SmartTOUCHCard

Ook is het mogelijk om de parameters in de SmartTOUCHReader te veranderen d.m.v. een ConfigKaart.

B. Functies van Configkaart

Behalve de parameters die invloed hebben op het uitlezen en beveiligen van een Configkaart zelf of de toegangscontrolegegevens, zijn er specifieke parameters die invloed hebben op de werking van de SmartTOUCH in het bijzonder. Deze worden hierna kort omschreven.

ENROLLCODE: Met deze code kan men bepalen welke EntrollCard bij welke lezers geldig zijn. Alleen als de Enrollcode in de lezer gelijk is aan de Entrollcode op de kaart zal de kaart werken bij de lezer.

ECVC: EnrollCard Version Control parameter. Deze parameter zorgt ervoor dat als een enrolkaart verloren is, deze verloren kaart ongeldig gemaakt kan worden door een nieuwe entrolkaart aan te maken met een hogere ECVC waarde. Als deze nieuwe kaart gelezen is, onthoudt de SmartTOUCH zodat alleen kaarten met een gelijke of hogere waarde geldig zijn.

CONCLUSIES

1. Systeem voor toegangscontrole en/of andere registraties van personen en/cf goederen; omvattende:

- een huis voorzien van sensormiddelen en eerste electronica
- identificatiemiddelen voorzien van tweede electronica voor draadloos contact met de in het huis aangebrachte electronica; en
- een orgaan voorzien van derde electronica voor draadloos contact met de in het huis aangebrachte electronica waarbij de derde electronica zodanig is ingericht en/of geprogrammeerd dat de eerste electronica kan worden geconfigureerd en/of ingesteld en/of gegevens vanuit de eerste electronica in de tweede electronica orgaan kunnen worden opgeslagen.

2. Systeem zoals conclusie 1, waarbij in of nabij het huis tevens aftastmiddelen voor het aftasten van een lichaamseigen gedeelte van een individu, bij voorkeur een vingerafdruk, zijn aangesloten.

3. Werkwijze waarbij gebruik wordt gemaakt van het systeem van conclusie 1 of 2.

4. Werkwijze gebruik makend van de belangrijkste elementen en of kenmerken van de bijgaande beschrijving.

5. Inrichting gebruik makend van de belangrijkste kenmerken en details van bijgaande beschrijving.